REMARKS

The Examiner has maintained the current rejection. As set forth below, such rejection is still deficient. However, despite such deficiencies and in the spirit of expediting the prosecution of the present application, applicant has incorporated the subject matter of multiple dependent claims into each of the independent claims. Since the subject matter of such dependent claims was already considered by the Examiner, it is asserted that such claim amendments would **not** require new search and/or consideration.

The Examiner has rejected Claims 1, 4, 7, 10, 11, 14, 19, 22, 25, 28, 29, and 32 under 35 U.S.C. 103(a) as being unpatentable over Tatebayashi, Key Distribution Protocol for Digital Mobile Communication Systems, in view of Mizikovsky, U.S. Patent No.: 5,748,734. The Examiner has further rejected Claims 2, 3, 5, 6, 8, 9, 12, 13, 15-18, 20, 21, 23, 24, 26, 27, 30, 31 and 33-39 under 35 U.S.C. 103(a) as being unpatentable over Tatebayashi in view of Mizikovsky in further view of Menezes. Applicant respectfully disagrees with these rejections, especially in view of the amendments made hereinabove.

With respect to the first element of the *prima facie* case of obviousness, the Examiner has responded to applicant's arguments by stating that they are not persuasive. First, the Examiner has stated that applicant's argument that it would have been unobvious to combine the teachings of Mizikovsky with the teachings of Tatebayashi is not persuasive because Mizikovsky discloses that the cryptographic key is generated at the base station and the wireless terminals. However, Mizikovsky's base station and wireless terminals only relate to communications between the base station and a single wireless terminal such that the key is only generated between seeds from the base station and single wireless terminal (see, specifically, Col. 7, line 37-Col. 8, line 13). Thus, since Mizikovsky does not teach any sort of first partial key value from a first node and second partial key value from a second node, in the manner claimed by applicant, it would not have been obvious to modify the teachings of Tatebayashi with the base station of Mizikovsky.

Again, applicant respectfully asserts that with respect to the first element of the *prima facie* case of obviousness, it would not have been obvious to one of ordinary skill in the art at the time the invention was made to the generate the common cryptographic key of Tatebayashi in the nodes as well as the network center in order to enhance the security of wireless communication infrastructure as taught in Mizikovsky. Applicant respectfully disagrees with this proposition, especially in view of the vast evidence to the contrary.

To emphasize, Tatebayashi suggests the establishment of a cryptographic key at a network center. See excerpt below.

> "The network center, in response to receiving the first ciphertext signal and the second ciphertext signal, decodes these as the first key-encryption-key signal and the second key-encryption-key, respectively, using a public-key-decoding device. Thus the network center has the first and second key-encryption-key signals r1 and r2. The network center then can encrypt the second key-encryption-key signal r2 with the first key-encryption-key signal r1 using the classical-key-encoding device, employing any type of classical encryption device." (See Section 3 - page 3, 4th paragraph)

This teaching is in direct contrast with applicant's claimed establishment of a cryptographic key at a second node. Thus, contrary to the Examiner's arguments, applicant's claimed feature would have been unobvious in view of Tatebayashi, since Tatebayashi *teaches away* from any sort of "establishing the cryptographic key at the second node using the first partial key value and a second partial key value created by the second node" (emphasis added), as claimed. *In re Hedges*, 783 F.2d 1038, 228 USPQ 685 (Fed. Cir. 1986).

With respect to the third element of the *prima facie* case of obviousness, applicant respectfully asserts that neither Tatebayashi nor Mizikovsky teach "establishing the

cryptographic key at the second node using the first partial key value and a second partial key value created by the second node" (see each of the independent claims). In particular, neither reference teaches the first partial key value being sent to the second node after being decrypted by the super node such that the second node can use, in part, the decrypted first partial key in establishing the cryptographic key (see applicant's specific claim language). In fact, Tatebayashi only teaches decoding after receiving both encryption keys. In addition, Mizikovsky only teaches communications between a network center and a terminal, but not between two terminals such that a second terminal receives a first partial key value in the manner claimed by applicant (see Col. 7).

Despite the foregoing and in the spirit of expediting the prosecution of the present application, applicant has now incorporated dependent Claims 2 et al. and 4 et al. into independent Claims 1 and 19 (the subject matter of Claim 2 et al. is incorporated in Claims 37 and 39 as originally filed and the subject matter of Claim 4 et al. is incorporated in Claim 39 as added in the last amendment).

The Examiner has responded to applicant's arguments with respect to dependent Claim 4 et al., presently incorporated into each of the independent claims, by stating that Tatebayashi teaches "sending a third message from the second node to the super node, wherein the third message includes the second partial key value encrypted using the public key belonging to the super node." Applicant disagrees with this assertion. Specifically, Tatebayashi only teaches that the network center decodes the first and second key-encryption key signals "in response to receiving the first ciphertext signal and the second ciphertext signal." Thus, Tatebayashi only teaches two messages, one sent from the first terminal to the network center and one sent from the second node to the network center. There is thus no third message, as claimed by applicant.

With respect to Claim 2 et al., presently incorporated into each of the independent claims, the Examiner has failed to provide any showing of applicant's claimed "sending a second message from the first node to the second node, wherein the second message includes a first message authentication code." Applicant respectfully asserts that none of

the references teach a second message including an authentication code, in the manner claimed by applicant.

To this end, applicant respectfully asserts that at least the first and third element of the *prima facie* case of obviousness have not been met, since the prior art reference fails to teach or suggest all the claim limitations, and it would not be unobvious to modify the prior art reference, as suggested by the Examiner. A notice of allowance or a specific prior art showing of each of the foregoing limitations, in combination with the remaining claim elements, is respectfully requested.

To this end, all of the pending independent claims are deemed allowable, along with any dependent claims dependent therefrom.

Reconsideration is respectfully requested.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. Applicants are enclosing a check to pay for the added claims. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P255).

Respectfully submitted,
Zilka-Kotab, PC

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100